

(13) (10)文献

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-339080

(43)Date of publication of application : 10.12.1999

(51)Int.Cl.

G07B 15/00

G07B 15/00

G06K 17/00

(21)Application number : 10-148074

(71)Applicant : MITSUBISHI HEAVY IND LTD

(22)Date of filing : 28.05.1998

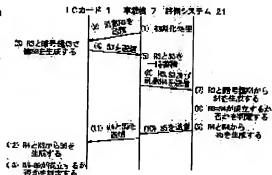
(72)Inventor : KATO MASAKI

## (54) SECURITY DEVICE OF TOLL COLLECTION DEVICE FOR TOLL ROAD

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a security device of the toll collection device for a toll road which can effectively prevent a cipher key group from being exposed.

**SOLUTION:** A moving-body-side controller is equipped with an IC card 1 and an on-vehicle machine 7 where the IC card is inserted and extracted. Here, the IC card 1 is stored with data representing a moving-body-side cipher key group K3 and a road-side controller 21 is stored with data representing a road-side cipher key group K4; and at least one of the road-side controller 2 and moving-body-side controller decides whether or not the moving-body-side cipher key group K3 and road-side cipher key group K4 match each other.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-339080

(43) 公開日 平成11年(1999)12月10日

(51) Int.Cl. <sup>8</sup>	識別記号	F I	
G 0 7 B 15/00		G 0 7 B 15/00	L
	5 1 0		5 1 0
G 0 6 K 17/00		G 0 6 K 17/00	T
			L

審査請求 未請求 請求項の数 6 O L (全 8 頁)

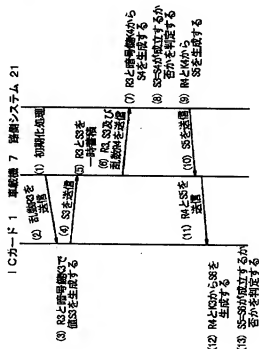
(21) 出願番号	特願平10-148074	(71) 出願人	000006208 三菱重工業株式会社 東京都千代田区丸の内二丁目5番1号
(22) 出願日	平成10年(1998)5月28日	(72) 発明者	加藤 聖樹 兵庫県神戸市兵庫区和田崎町一丁目1番1号 三菱重工業株式会社神戸造船所内
		(74) 代理人	弁理士 工藤 実 (外1名)

(54) 【発明の名称】 有料道路の料金収受装置におけるセキュリティ装置

(57) 【要約】

【課題】 暗号鍵群の暴露を有効に防止することができる有料道路の料金収受装置におけるセキュリティ装置を提供する

【解決手段】 移動体側制御装置 7 A は、I C カード 1 と、前記 I C カードが挿脱される車載機 7 とを備え、前記 I C カードに移動体側暗号鍵群 K 3 を示すデータが格納され、道路側制御装置 2 1 に道路側暗号鍵群 K 4 を示すデータが格納され、前記道路側制御装置および前記移動体側制御装置の少なくとも一方は、前記移動体側暗号鍵群と前記道路側暗号鍵群が一致しているか否かを判定する。



【特許請求の範囲】

【請求項1】 相互に通信可能な道路側制御装置（21）および移動体側制御装置（7A）とを備えてなる有料道路の料金収受装置におけるセキュリティ装置であって、

前記移動体側制御装置（7A）は、

ICカード（1）と、

前記ICカード（1）が挿脱される車載機（7）とを備え、

前記ICカード（1）に移動体側暗号鍵群（K3）を示すデータが格納され、

前記道路側制御装置（21）に道路側暗号鍵群（K4）を示すデータが格納され、

前記道路側制御装置（21）および前記移動体側制御装置（7A）の少なくとも一方は、前記移動体側暗号鍵群（K3）と前記道路側暗号鍵群（K4）が一致しているか否かを判定する（ステップS8、ステップS13）有料道路の料金収受装置におけるセキュリティ装置。

【請求項2】 請求項1記載の有料道路の料金収受装置におけるセキュリティ装置において、

前記移動体側制御装置（7A）は、暗号化情報（R3、R4）を発生する暗号化情報発生手段と、

前記暗号化情報発生手段が発生した前記暗号化情報（R3）を示すデータおよび前記移動体側暗号鍵群（K3）を示すデータを用いて第1の生成情報（S3）を生成する（ステップS3）ための移動体側演算処理手段（2）とを備えてなり、

前記道路側制御装置（21）は、前記移動体側制御装置（7A）と通信して入手した前記暗号化情報（R3）を示すデータ、および前記道路側暗号鍵群（K4）を示すデータを用いて第2の生成情報（S4）を生成する（ステップS7）ための道路側演算処理手段を備えてなり、

前記道路側制御装置（21）および前記移動体側制御装置（7A）の少なくとも一方は、前記移動体側暗号鍵群（K3）と前記道路側暗号鍵群（K4）が一致しているか否かを判定するときに、前記第1の生成情報（S3）を示すデータと前記第2の生成情報（S4）を示すデータとが一致しているか否かを判定する（ステップS8）有料道路の料金収受装置におけるセキュリティ装置。

【請求項3】 請求項1記載の有料道路の料金収受装置におけるセキュリティ装置において、

前記移動体側制御装置（7A）は、暗号化情報（R3、R4）を発生する暗号化情報発生手段と、

移動体側演算処理手段（2）とを備えてなり、

前記道路側制御装置（21）は、道路側演算処理手段を備えてなり、

前記移動体側制御装置（7A）は、

前記暗号化情報発生手段により発生させた第1の前記暗号化情報（R3、ステップS2）を示すデータと、

前記第1の暗号化情報（R3）を示すデータと前記移動体側暗号鍵群（K3）を示すデータとを用いて前記移動体側演算処理手段（2）により生成させた第1の生成情報（S3、ステップS3）を示すデータと、

前記暗号化情報発生手段により発生させた第2の前記暗号化情報（R4）を示すデータと、前記道路側制御装置（21）に送信し（ステップS6）、

前記道路側制御装置（21）は、前記第1の暗号化情報（R3）を示すデータと前記道路側暗号鍵群（K4）を示すデータとを用いて前記道路側演算処理手段により第2の生成情報（S4）を生成し（ステップS7）、

かつ、前記第1の生成情報（S3）と前記第2の生成情報（S4）とが一致しているか否かを判定して前記道路側暗号鍵群（K4）を示すデータと前記移動体側暗号鍵群（K3）を示すデータとが一致しているか否かの第1の認証を行い（ステップS8）、

かつ、前記第2の暗号化情報（R4）を示すデータと前記道路側暗号鍵群（K4）を示すデータとを用いて前記道路側演算処理手段により第3の生成情報（S5）を生成し（ステップS9）、

かつ、前記第3の生成情報（S5）を示すデータを前記移動体側制御装置（7A）に送信し（ステップS10）、

前記移動体側制御装置（7A）は、前記第2の暗号化情報（R4）を示すデータと前記移動体側暗号鍵群（K3）を示すデータとを用いて前記移動体側演算処理手段（2）により第4の生成情報（S6）を生成し（ステップS12）、

かつ、前記第4の生成情報（S6）と前記第3の生成情報（S5）とが一致しているか否かを判定して、前記移動体側暗号鍵群（K3）を示すデータと前記道路側暗号鍵群（K4）を示すデータとが一致しているか否かの第2の認証を行う（ステップS13）有料道路の料金収受装置におけるセキュリティ装置。

【請求項4】 請求項1から3のいずれかに記載の有料道路の料金収受装置におけるセキュリティ装置において、

前記移動体側暗号鍵群（K3）を示すデータは、前記移動体側制御装置（7A）のうち前記ICカード（1）にのみ格納されている有料道路の料金収受装置におけるセキュリティ装置。

【請求項5】 請求項2から4のいずれかに記載の有料道路の料金収受装置におけるセキュリティ装置において、

前記移動体側演算処理手段（2）は、前記ICカード（1）に備えられている有料道路の料金収受装置におけるセキュリティ装置。

【請求項6】 請求項3から5のいずれかに記載の有料

道路の料金収受装置におけるセキュリティ装置において、

前記第2の認証は、前記ICカード(1)で行われる有料道路の料金収受装置におけるセキュリティ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、有料道路の料金収受装置におけるセキュリティ装置に関する。

【0002】

【従来の技術】有料道路では、料金収受がゲートで行われる。各自動車は、料金収受のために減速しゲートで停止し、料金収受の後に再び加速する。このような加速減速は、交通渋滞を招くだけでなく、燃料消費量と廃棄ガスを増大させる。このような加速減速を不要するために、料金収受をノンストップで行う試みがなされている。

【0003】これは、無線通信機能を持つ車載機を車両に搭載し、この車載機と、料金所に整備された路上機アンテナとの間で、料金収受を行うものである。図3を参照して、上記料金収受システムの一例を説明する。

【0004】図3に示すように、料金収受システムは、道路側制御システム68と、移動体側制御システム53Aとを備えている。道路側制御システム68は、第1のアンテナ58と、第1のアンテナコントロール59と、第2のアンテナ60と、第2のアンテナコントロール61と、車両検知センサ62と、車両検知センサコントロール63と、不正防止カメラ64と、不正防止カメラコントロール65と、これらのコントロール59、61、63、65を統括してコントロールする道路側コントロール66とを備えている。道路側制御システム68は、公衆回線または専用回線にて中央制御システム67に接続されている。

【0005】移動体側制御システム53Aは、車載機53と、ICカード50とを備えている。ICカード50は、メモリ52と、CPU51とを備えている。車載機53は、ICカードスロット56と、CPU55と、RFユニット54と、メモリ57とを備えている。車載機53は、さらに表示ディスプレイ、ボタン、LED表示器等のヒューマンI/F(図示せず)を備えている。

【0006】車載機53のメモリ57およびICカード50のメモリ52には、それぞれ、所定の暗号鍵または暗号鍵群(以下、単に暗号鍵群と記す)が格納されている。

【0007】次に、上記料金収受システムにおけるセキュリティシステムについて説明する。ここで、セキュリティシステムとは、ICカード50、車載機53および道路側制御システム68の偽造を防止するために、相互に認証を行うシステムをいう。上記のセキュリティシステムでは、車載機53のメモリ57に格納された暗号鍵群(「K2」とする)と、ICカード50のメモリ52に

格納された暗号鍵群(「K1」とする)との一致が、車載機53とICカード50との双方で認証される。

【0008】このような暗号鍵群K1、K2の一致の相互認証の結果は、車載機53から第1のアンテナ58に送信される。相互認証が成立すれば、料金収受の手続きが道路側制御システム68と移動体側制御システム53Aとの間で行われる。相互認証が成立しなかった場合は、不正防止カメラ64により、その当該車載機53を搭載した車を不正車両として撮影するようになっている。なお、車両検知センサ62は、相互認証が成立しない場合に、当該車両の通過を検知して不正防止カメラ64を起動するためのものである。

【0009】次に、図4を参照して、上記セキュリティシステムにおける相互認証の手順を、(1)から(10)のステップに分けて説明する。

【0010】(1)まず、車載機53は、ICカード50がICカードスロット56に挿入された時点で、ICカード50に乱数R1を送信する。

(2)ICカード50は、その乱数R1とメモリ52に格納された暗号鍵群K1で、値S1を作成する。数式表現では以下ようになる。

$S1 = f(R1, K1) \dots\dots\dots (式1)$ 。

【0011】(3)ICカード50は、値S1を車載機53に送り返す。

(4)車載機53は、乱数R1とメモリ57に格納された暗号鍵群K2を使用して、式(1)と同じ計算を行い、値S2を求める。数式表現では以下ようになる。

$S2 = f(R1, K2) \dots\dots\dots (式2)$ 。

(5)この結果、ICカード50のメモリ52に内蔵された暗号鍵群K1と、車載機53のメモリ57に内蔵された暗号鍵群K2が同じ値であれば、その結果、 $S1 = S2$ 、となるはずである。したがって、車載機53は、 $S1 = S2$ 、が成立するか否かを判定し、これが一致した場合には、ICカード50が同じ暗号鍵群を有する(K1=K2)カードであるとして、ICカード50の正当性を確認することになる。

【0012】(6)次に、ICカード50は、乱数R2を発生させて、車載機53に送信する。

(7)車載機53は、その乱数R2を使用して以下の計算を実行する。

$S3 = f(R2, K2) \dots\dots\dots (式3)$ 。

(8)値S3は、車載機53からICカード50に送信される。

【0013】(9)ICカード50では、以下の計算を行い、値S4を求める。

$S4 = f(R2, K1) \dots\dots\dots (式4)$ 。

(10)ICカード50は、式(3)、式(4)、が成立するか否かを判定し、値S3と値S4が等しい場合に限り、車載機53と同じ暗号鍵群を共有する(K1=K2)ものとして、車載機53の正当性を確認する。

【0014】上記(1)から(10)のステップの結果として、ICカード50と車載機53の相互認証が成立することとなる。

【0015】上記において、暗号化に使用される暗号鍵群K1、K2に含まれる暗号鍵の数は、1つでなくともよく、複数使用することができる。いずれにしても、ICカード50および車載機53の各々は、同一の暗号鍵または同一の暗号鍵群を共有する必要がある。

【0016】

【発明が解決しようとする課題】ところで、上記のような料金収受システムでは、ICカード50および車載機53の各々が同一の暗号鍵群K1、K2を共有している。したがって、仮に車載機53が分解されてメモリ57の暗号鍵群K2が解析された場合には、車載機53自体の偽造が可能となるのみならず、同じ暗号鍵群を共有するICカード50の暗号鍵群K1も暴露されることになり、ICカード50の偽造も可能になってしまうという問題がある。このような偽造を防止することが要請されている。

【0017】本発明は、このような技術的背景に基づいてなされたものであり、次のような課題を解決するものである。本発明の目的は、暗号鍵群の暴露を防止することができる有料道路の料金収受装置におけるセキュリティ装置を提供することにある。本発明の他の目的は、ICカードまたは車載機の偽造を防止することができる有料道路の料金収受装置におけるセキュリティ装置を提供することにある。本発明の更に他の目的は、数量が限定されセキュリティの管理が容易な有料道路の料金収受装置におけるセキュリティ装置を提供することにある。

【0018】

【課題を解決するための手段】本発明の有料道路の料金収受装置におけるセキュリティ装置は、相互に通信可能な道路側制御装置および移動体側制御装置とを備えてなる有料道路の料金収受装置におけるセキュリティ装置であって、前記移動体側制御装置は、ICカードと、前記ICカードが挿脱される車載機とを備え、前記ICカードに移動体側暗号鍵群を示すデータが格納され、前記道路側制御装置に道路暗号鍵群を示すデータが格納され、前記道路側制御装置および前記移動体側制御装置の少なくとも一方は、前記移動体側暗号鍵群と前記道路側暗号鍵群が一致しているか否かを判定する。

【0019】本発明の有料道路の料金収受装置におけるセキュリティ装置は、請求項1記載の有料道路の料金収受装置におけるセキュリティ装置において、前記移動体側制御装置は、暗号化情報が発生する暗号化情報発生手段と、前記暗号化情報発生手段が発生した前記暗号化情報を用いて第1の生成情報を作成するための移動体側演算処理手段とを備えてなり、前記道路側制御装置は、前記移動体側制御装置と通信して入手した前記暗号化情報

を示すデータ、および前記道路側暗号鍵群を示すデータを用いて第2の生成情報を作成するための道路側演算処理手段を備えてなり、前記道路側制御装置および前記移動体側制御装置の少なくとも一方は、前記移動体側暗号鍵群と前記道路側暗号鍵群が一致しているか否かを判定するときに、前記第1の生成情報を示すデータと前記第2の生成情報を示すデータとが一致しているか否かを判定する。

【0020】本発明の有料道路の料金収受装置におけるセキュリティ装置は、請求項1記載の有料道路の料金収受装置におけるセキュリティ装置において、前記移動体側制御装置は、暗号化情報が発生する暗号化情報発生手段と、移動体側演算処理手段とを備えてなり、前記道路側制御装置は、道路側演算処理手段を備えてなり、前記移動体側制御装置は、前記暗号化情報発生手段により発生させた第1の前記暗号化情報を示すデータと、前記第1の暗号化情報を示すデータと前記移動体側暗号鍵群を示すデータとを用いて前記移動体側演算処理手段により生成させた第1の生成情報を示すデータと、前記暗号化情報発生手段により発生させた第2の前記暗号化情報を示すデータと、前記道路側制御装置に送信し、前記道路側制御装置は、前記第1の暗号化情報を示すデータと前記道路側暗号鍵群を示すデータとを用いて前記道路側演算処理手段により第2の生成情報を作成し、かつ、前記第1の生成情報と前記第2の生成情報とが一致しているか否かを判定して前記道路側暗号鍵群を示すデータと前記第2の暗号化情報を用いて前記道路側演算処理手段により第3の生成情報を作成し、かつ、前記第3の生成情報を示すデータを前記移動体側制御装置に送信し、前記移動体側制御装置は、前記第2の暗号化情報を示すデータと前記移動体側暗号鍵群を示すデータとを用いて前記移動体側演算処理手段により第4の生成情報を作成し、かつ、前記第4の生成情報と前記第3の生成情報とが一致しているか否かを判定して、前記移動体側暗号鍵群を示すデータと前記道路側暗号鍵群を示すデータとが一致しているか否かの第2の認証を行う。

【0021】本発明の有料道路の料金収受装置におけるセキュリティ装置は、請求項1から3のいずれかに記載の有料道路の料金収受装置におけるセキュリティ装置において、前記移動体側暗号鍵群を示すデータは、前記移動体側制御装置のうち前記ICカードにのみ格納されている。

【0022】本発明の有料道路の料金収受装置におけるセキュリティ装置は、請求項2から4のいずれかに記載の有料道路の料金収受装置におけるセキュリティ装置において、前記移動体側演算処理手段は、前記ICカードに備えられている。

【0023】本発明の有料道路の料金収受装置におけるセキュリティ装置は、請求項3から5のいずれかに記載の有料道路の料金収受装置におけるセキュリティ装置において、前記第2の認証は、前記ICカードで行われる。

【0024】上記のように、ICカードに秘密情報を集め、ICカードで論理演算を行うことにより、更に、ICカードの偽造が困難になる。移動体側と固定側との間で必要十分条件を満たす相互の暗号固定化を行うためには、固定側の複雑な装置の中から秘密情報を盗む必要があるが、固定側装置の管理を厳格に行うことが可能であるから、暗号鍵群の暴露はほとんど不可能になる。ICカードが盗まれた場合には、ただちに届け出を固定側装置の制御装置に対して行うことができるから、その偽造は実質的に不可能である。

【0025】

【発明の実施の形態】以下、添付図面を参照して、本発明の有料道路の料金収受装置におけるセキュリティ装置の一実施の形態を説明する。

【0026】図1は、本実施形態の装置ブロック図である。図1に示すように、本セキュリティシステムは、道路側制御システム21と、移動体側制御システム7Aとを備えている。道路側制御システム21は、第1のアンテナ9を備えている。第1のアンテナ9は、第1のアンテナコントローラ10によりその送受信が制御されている。第1のアンテナコントローラ10には、道路側第1のメモリ11が設けられている。この道路側第1のメモリ11は、道路側暗号鍵群K4を格納している。

【0027】道路側制御システム21は、さらに、第2のアンテナ12を備えている。第2のアンテナ12は、第2のアンテナコントローラ13によりその送受信が制御されている。第2のアンテナコントローラ13には、道路側第2のメモリ14が設けられている。道路側第2のメモリ14は、道路側第1のメモリ11と同様に、道路側暗号鍵群K4を格納している。

【0028】第1のアンテナ9と、第1のアンテナコントローラ10と、道路側第1のメモリ11は、第1道路側認証用ユニットを形成する。第2のアンテナ12と、第2のアンテナコントローラ13と、道路側第2のメモリ14は、第2道路側認証用ユニットを形成する。このように第1道路側認証用ユニットと第2道路側認証用ユニットは、例えば、有料道路の上り線用と下り線用として、または、出口用と入口用として、近接位置にまたは離隔位置に配置される。

【0029】道路側制御システム21は、さらに、車両検知センサ15、車両検知センサコントローラ16、不正防止カメラ17、不正防止カメラコントローラ18およびこれら諸機器を統一してコントロールするための道路側コントローラ19を備えている。道路側コントローラ19は各ゲートにそれぞれ配置され、これら複数の道

路側コントローラ19は、全体として中央制御システム20により群管理が行われる。例えば、後述するICカード1の盗難時には、そのカード番号が中央制御システム20を介して複数の道路側制御システム21に伝達される。

【0030】移動体側制御システム7Aは、ICカード1と車載機7とを備えている。ICカード1は、CPU2とメモリ3とを備えている。メモリ3は、移動体側暗号鍵群K3を記憶しこれが更新されない限り永久的に保存している。車載機7は、ICカードスロット6、CPU5およびRFユニット4を備えている。

【0031】車載機7は、移動体側暗号鍵群K3を保存していない。ここで、「移動体側暗号鍵群K3を保存していない」という意味について説明する。移動体側暗号鍵群K3は、N個の移動体側暗号鍵群K31……K3Nの群でよい。この場合、車載機7は、移動体側暗号鍵群K31……K3Nのうちどの1つも保有していないということである。群の要素が1つの場合にも、それは群または集合である、という。

【0032】次に、図2を参照して、本実施形態のセキュリティシステムについて説明する。ICカード1は、車載機7のICカードスロット6に挿入される。この挿入により、ICカード1と車載機7は、初期化が行われる(図2においてステップ(1)参照。なお、以下、ステップ(1)は「ステップS1」、ステップ(2)は「ステップS2」……と称する)。

【0033】車載機7は、第1移動体側暗号化情報R3を発生させる。ここで、前記暗号化情報は、例えば、乱数である。第1移動体側暗号化情報R3は、ICカード1のCPU2に送信される(ステップS2参照)。CPU2は、メモリ3に格納された移動体側暗号鍵群K3と第1移動体側暗号化情報R3とを用いて、次に示される演算計算を行って生成値S3を生成する(ステップS3参照)。

$S3 = f(R3, K3) \dots\dots\dots (式5)$

【0034】次いで、ステップS4に示すように、ICカード1は、値S3を車載機7に送り返す。第1移動体側暗号化情報R3と値S3は、車載機7に一時的に記憶される(ステップS5参照)。これらの値は、本セキュリティシステムの動作完了後には、車載機7からは消去される。車載機7の破壊によりICカード1の偽造に必要な情報が盗用されるのを未然に防止するためである(この意味については後述する)。

【0035】車載機7が道路側制御システム21との通信可能領域に入ると、車載機7と道路側制御システム21との間で双方向にデータをやり取りするための無線通信が行われる。すなわち、ステップS6に示すように、車載機7は、前記蓄積されているデータ(第1移動体側暗号化情報R3および、ICカード1で計算された生成値S3)と、車載機7で発生させる第2移動体側暗号化

情報R4を、第1のアンテナ9に送信する。これらの3つのデータR3、S3、R4は、第1のアンテナコントロール10に送られる。

【0036】ステップS7に示すように、第1のアンテナコントロール10は、第1移動体側暗号化情報R3と、メモリ11に格納されている道路側暗号鍵群K4とを使用して、式(1)と同形の演算計算を行い生成値S4を求める。

$S4 = f(R3, K4) \dots\dots (式6)$

【0037】次いで、ステップS8に示すように、S3 = S4、の関係が成立するか否かを判定する。成立すると判定されれば、第1のアンテナコントロール10は、道路側第1のメモリ11とICカード1が、同一または共通の暗号鍵を共有する(K3 = K4)ものとして、両側システムの同定を確認して、ICカード1の正当性を確認・認証してよいことになる。

【0038】次に、ステップS9に示すように、第1のアンテナコントロール10は、第2移動体側暗号化情報R4と、道路側暗号鍵群K4を使用して、次の計算を行う。

$S5 = f(R4, K4) \dots\dots (式7)$

【0039】この生成値S5は、第1のアンテナ9を介して車載機7に送信される(ステップS10)。次いで、ステップS11に示すように、車載機7は、第2移動体側暗号化情報R4と生成値S5とをICカード1に送信する。

【0040】次に、ICカード1は、次の計算を実行する(ステップS12)。

$S6 = f(R4, K3) \dots\dots (式8)$

この結果、S5 = S6の関係が成立するか否かが判定されて(ステップS13)、成立していれば、ICカード1は、道路側第1のメモリ11とICカード1が同一または共通の暗号鍵群を共有する(K3 = K4)ものとして、両側システムの同定を確認して、道路側制御システム21の全体の正当性を確認・認証してよいことになる。この認証結果は、車載機7を介して第2のアンテナ12に送信されることになる。

【0041】上記のように、本実施形態では、ICカード1と同一または共通の暗号鍵群を共有するものは、車載機7ではなく、道路側制御システム21である。したがって、道路側制御システム21を破壊等して暗号鍵群K4を解析しない限り、ICカード1を持たない第三者にICカード1の暗号鍵群K3が暴露されることはない。したがって、不特定多数存在し盗難等の管理を行い難い車載機7に、暗号鍵群K4を記憶させておく場合に比べて、本実施形態は、ICカード1の偽造防止に有効である。

【0042】すなわち、暗号鍵群K4が道路側制御システム21に記憶されている以上、相互認証を行うに限りては、道路側制御システム21が必須となる。このこと

から、ICカード1が行う計算である式(8)(図2のステップS12)についても、道路側制御システム21自らが、ICカード1と車載機7とを利用して計算したことに等価であるといえる。言い換えると、相互認証は、道路側制御システム21により確認されたことになる。セキュリティの管理の観点から、道路側制御システム21による確認は、従来の車載機による確認の場合に比べて、相互認証の精度も向上する。例えば、車載機は、道路側制御装置21に比べて改造し易く、その場合、暗号鍵群が不一致の場合にも一致との認識を与えるように改造することも考えられる。これに対して、本実施形態の道路側制御装置21の改造は、考えにくく、犯罪防止に有効である。

【0043】第1のアンテナ9と第2のアンテナ12の両方の使用により、駐車場の入口処理と出口処理とに分けることも可能である。既述の演算計算を含む処理の時間が十分にあれば、第1のアンテナ9だけで実行することが可能である。さらには、逆方向走行車両の処理を併行させることも可能である。

【0044】以上に述べたように、本実施形態によれば、不特定多数に供給される車載機7ではなく、数量限定され、さらにセキュリティ面においても管理が容易な道路側制御システム21内のアンテナコントロール10、13だけに暗号鍵群K4を格納することにより、ICカード1と共有された暗号鍵群K4の解読を困難にすることができ、ICカードの偽造を未然に防止することができ。

【0045】さらに、新規の暗号鍵群を有したICカードが発行された場合でも、道路側制御システム内のメモリ11、14に格納された暗号鍵群を更新するのみでよく、不特定多数に供給された車載機7に格納された暗号鍵群を更新する場合と比較して、格段に容易にすることができ。さらにまた、車載機7は、暗号鍵群を安全に格納するメモリを有したり、暗号化のアルゴリズムを有する必要があるため、車載機7を非常に安価に構成することができるようになる。

【0046】

【発明の効果】本発明による有料道路の料金収受装置におけるセキュリティ装置によれば、相互に通信可能な道路側制御装置および移動体側制御装置とを備えてなる有料道路の料金収受装置におけるセキュリティ装置であって、前記移動体側制御装置は、ICカードと、前記ICカードが挿脱される車載機とを備え、前記ICカードに移動体側暗号鍵群を示すデータが格納され、前記道路側制御装置に道路側暗号鍵群を示すデータが格納され、前記道路側制御装置および前記移動体側制御装置の少なくとも一方は、前記移動体側暗号鍵群と前記道路側暗号鍵群が一致しているか否かを判定することから、前記移動体側暗号鍵群は、前記車載機に代えて前記ICカードに保存され、またさらに、前記移動体側暗号鍵群と同一な

(共通する)前記道路側暗号鍵群は、前記道路側制御システムにしか保存されておらず、前記移動体暗号鍵群について、前記ICカードを持たない第三者が知り得る可能性を最小限に抑えることができ、前記ICカードの偽造を有効に防止することができる。

【図面の簡単な説明】

【図1】図1は、本発明の有料道路の料金収受装置におけるセキュリティ装置の一実施形態を示す装置ブロック図である。

【図2】図2は、本実施形態において行われる認証手続きの流れを示す図である。

【図3】図3は、一般の有料道路の料金収受装置におけるセキュリティ装置を示す装置ブロック図である。

【図4】図4は、一般の有料道路の料金収受装置におけるセキュリティ装置において行われる認証手続きの流れを示す図である。

【符号の説明】

1…ICカード

2…CPU(カード側)

3…メモリ

\*5…CPU(車載機側)

7…車載機

7A…移動体側制御装置(移動体側制御システム)

9…第1のアンテナ

10…第1のアンテナコントローラ

11…道路側第1のメモリ

12…第2のアンテナ

13…第2のアンテナコントローラ

14…道路側第2のメモリ

19…道路側コントローラ

20…中央制御システム

21…道路側制御装置(道路側制御システム)

K3…移動体側暗号鍵群

K4…道路側暗号鍵群

R3…第1の暗号化情報

R4…第2の暗号化情報

S3…第1の生成情報

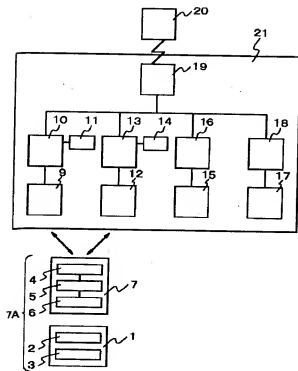
S4…第2の生成情報

S5…第3の生成情報

S6…第4の生成情報

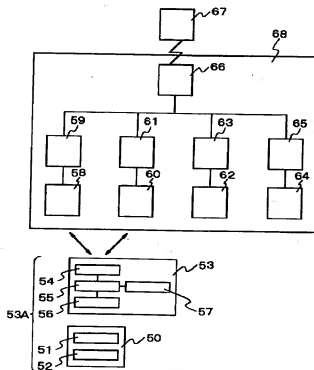
\*20

【図1】



本発明の料金収受システム

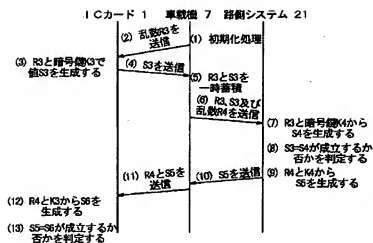
【図3】



従来の料金収受システム



【図2】



【図4】

